IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for establishing a cryptographic key between a first node and a second node, comprising:

sending a first message from the first node to the second node, wherein the first message requests establishing the cryptographic key;

sending a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, a second node identifier for the second node, and a message authentication code created using a second node key belonging to the second node;

recreating the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center;

verifying at the key distribution center the message authentication code in the second message using the second node key; and

if the message authentication code is verified,

creating the cryptographic key at the key distribution center, and

communicating the cryptographic key to the second node and the first node;

wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar;

wherein communicating the cryptographic key to the second node and the first node includes:

encrypting a hash value and the cryptographic key using the second node key to create a first encrypted key;

recreating a first node key belonging to the first node, wherein the first node key was previously created using the secret key and the first node identifier;

encrypting the hash value and the cryptographic key using the first node key to create a second encrypted key;

sending a third message from the key distribution center to the second node, wherein the third message includes the first encrypted key and the second encrypted key;

decrypting at the second node the first encrypted key from the third message to recover the hash value and the cryptographic key;

verifying the hash value; and

if the hash value is verified,

sending a fourth message to the first node from the second node, wherein the fourth message includes the second encrypted key and a key confirmation value so that the first node can confirm that the cryptographic key has been established,

decrypting at the first node the second encrypted key from the fourth message to recover the hash value and the cryptographic key,

verifying the hash value,

establishing at the first node that the second node has the cryptographic key, and

if the hash value is verified and it is established at the first node that the second node has the cryptographic key,

sending a fifth message to the second node from the first node so that the second node can confirm that the cryptographic key has been established.

2. (Cancelled)

3. (Currently Amended) The method of claim [2]1, wherein the first message includes the first node identifier, the second node identifier, a third identifier for the key distribution center, and a first nonce, wherein a nonce is a random number selected for message confirmation purposes that has a statistically low probability of being reused.

4. (Original) The method of claim 3, wherein the second message includes the third identifier, the second node identifier, the first node identifier, a second nonce, the first nonce, and the message authentication code, wherein the message authentication code is created from the third identifier, the second node identifier, the first node identifier, the second nonce, and the first nonce.

5. (Original) The method of claim 4, wherein verifying the message authentication code includes:

creating a test message authentication code from the third identifier, the second node identifier, the first node identifier, the second nonce, and the first nonce using the second node key; and

comparing the test message authentication code with the message authentication code.

6. (Original) The method of claim 5, wherein the hash value is created from the second node identifier, the first node identifier, the second nonce, and the first nonce.

7. (Original) The method of claim 6, wherein the third message includes the second node identifier, the first node identifier, the second encrypted key, and the first encrypted key.

8. (Original) The method of claim 7, wherein validating the hash value at the second node includes:

creating a first test hash value from the second node identifier, the first node identifier, the second nonce, and the first nonce; and

comparing the first test hash value with the hash value.

9. (Original) The method of claim 8, wherein the fourth message includes the first node identifier, the second node identifier, the second nonce, the first encrypted key, and a first confirmation value, wherein the first confirmation value has been encrypted with the cryptographic key.

10. (Original) The method of claim 9, wherein the first confirmation value includes the second nonce and the first nonce.

11. (Previously Amended) The method of claim 10, wherein verifying the hash value includes:

creating a second test hash value from the second node identifier, the first node identifier, the second nonce, and the first nonce; and

comparing the second test hash value with the hash value.

12. (Original) The method of claim 11, wherein establishing at the first node that the second node has the cryptographic key includes:

decrypting the first confirmation value using the cryptographic key; and

verifying that the first nonce is what was sent in the first message.

13. (Original) The method of claim 12, wherein the fifth message includes:

the second node identifier, the first node identifier, and a second confirmation value.

14. (Original) The method of claim 13, wherein creating the second confirmation value at the first node includes:

reordering the first nonce and the second nonce recovered by decrypting the first confirmation value to create the second confirmation value; and

encrypting the second confirmation value using the cryptographic key.

15. (Original) The method of claim 14, wherein confirming at the second node that the cryptographic key has been established includes:

decrypting the second confirmation value using the cryptographic key; and

verifying that the second nonce was sent in the second message.

16. (Original) The method of claim 1, further comprising:

creating the second node key, wherein the second node key is created using the secret key and the second node identifier; and

installing the second node key into the second node prior to deployment of the second node.

17. (Currently Amended) The method of claim [2]1, further comprising:

creating the first node key, wherein the first node key is created using the secret key and the first node identifier; and

installing the first node key into the first node prior to deployment of the first node.

18. (Currently Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for establishing a cryptographic key between a first node and a second node, the method comprising:

sending a first message from the first node to the second node, wherein the first message requests establishing the cryptographic key;

sending a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, a

second node identifier for the second node, and a message authentication code created using a second node key belonging to the second node;

recreating the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center;

verifying at the key distribution center the message authentication code in the second message using the second node key; and

if the message authentication code is verified,

creating the cryptographic key at the key distribution center, and

communicating the cryptographic key to the second node and the first node;

wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar;

wherein communicating the cryptographic key to the second node and the first node includes:

encrypting a hash value and the cryptographic key using the second node key to create a first encrypted key;

recreating a first node key belonging to the first node, wherein the first node key was previously created using the secret key and the first node identifier;

encrypting the hash value and the cryptographic key using the first node key to create a second encrypted key;

sending a third message from the key distribution center to the second node, wherein the third message includes the first encrypted key and the second encrypted key;

decrypting at the second node the first encrypted key from the third message to recover the hash value and the cryptographic key;

verifying the hash value; and

if the hash value is verified,

sending a fourth message to the first node from the second node, wherein the fourth message includes the second encrypted key,

decrypting at the first node the second encrypted key from the fourth message to recover the hash value and the cryptographic key,

verifying the hash value,

establishing at the first node that the second node has the cryptographic key, and

if the hash value is verified and it is established at the first node that the second node has the cryptographic key,

sending a fifth message to the second node from the first node so that the second node can confirm that the cryptographic key has been established.

19. (Cancelled)

20. (Currently Amended) An apparatus that facilitates establishing a cryptographic key between a first node and a second node, comprising:

a first sending mechanism that is configured to send a first message from the first node to the second node, wherein the first message requests establishing the cryptographic key;

a second sending mechanism that is configured to send a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, a second node identifier for the second node, and a message authentication code created using a second node key belonging to the second node;

a key recreating mechanism that is configured to recreate the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center;

a first verifying mechanism at the key distribution center that is configured to verify the message authentication code in the second message using the second node key;

a creating mechanism that is configured to create the cryptographic key at the key distribution center; ~~and~~

a communicating mechanism that is configured to communicate the cryptographic key to the second node and the first node;

an encrypting mechanism that is configured to encrypt a hash value and the cryptographic key using the second node key to create a first encrypted key;

the key recreating mechanism that is further configured to recreate a first node key belonging to the first node, wherein the first node key was previously created using the secret key and the first node identifier;

the encrypting mechanism that is further configured to encrypt the hash value and the cryptographic key using the first node key to create a second encrypted key;

a third sending mechanism that is configured to send a third message from the key distribution center to the second node, wherein the third message includes the first encrypted key and the second encrypted key;

a first decrypting mechanism at the second node that is configured to decrypt the first encrypted key from the third message to recover the hash value and the cryptographic key;

a second verifying mechanism that is configured to verify the hash value; and

the second sending mechanism that is further configured to send a fourth message to the first node from the second node, wherein the fourth message includes the second encrypted key,

a second decrypting mechanism at the first node that is configured to decrypt the second encrypted key from the fourth message to recover the hash value and the cryptographic key,

a third verifying mechanism that is configured to verify the hash value,

an establishing mechanism at the first node that is configured to establish that the second node has the cryptographic key, and

the first sending mechanism that is further configured to send a fifth message to the second node from the first node so that the second node can confirm that the cryptographic key has been established;

wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar.

21. (Cancelled)